Information Assurance and Critical Infrastructure Protection

"A Federal Perspective"

Presented by the

Government Electronics and Information Technology Association

2001

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
01-01-2001		xx-xx-2001 to xx-xx-2001

4. TITLE AND SUBTITLE
Information Assurance and Critical Infrastructure Protection "A Federal Perspective"
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
Government Electronics and Information Technology
2500 Wilson Blvd.
Arlington, VA22201-3834

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The Internet and associated electronic communications have become an indispensable tool for both business and government. This technology allows organizations to conduct electronic commerce, provide better customer service, collaborate with remote partners, reduce communications costs, improve internal communication and access needed information rapidly. However, our reliance on a networked electronic society is not risk free. Security breaches, theft of proprietary information, privacy risk, financial fraud, and sabotage of data or networks are emerging threats in our new information age. Both the number and sophistication of attacks on our information infrastructure have exponentially increased in the last decade. In fact, there have been more reported incidents of network attack in the last quarter of 2000 than in the entire previous year.

15. SUBJECT TERMS
IATAC COLLECTION; information assurance; networks; systems; security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	8	Fenster, Lynn lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	1/1/2001	Report 1/1/2001

4. TITLE AND SUBTITLE
Information Assurance and Critical Infrastructure Protection "A Federal Perspective"

5. FUNDING NUMBERS

6. AUTHOR(S)
Unknown

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Government Electronics and Information Technology
2500 Wilson Boulevard, Arlington, VA 22201-3834

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

The Internet and associated electronic communications have become an indispensable tool for both business and government. This technology allows organizations to conduct electronic commerce, provide better customer service, collaborate with remote partners, reduce communications costs, improve internal communication and access needed information rapidly. However, our reliance on a networked electronic society is not risk free. Security breaches, theft of proprietary information, privacy risk, financial fraud, and sabotage of data or networks are emerging threats in our new information age. Both the number and sophistication of attacks on our information infrastructure have exponentially increased in the last decade. In fact, there have been more reported incidents of network attack in the last quarter of 2000 than in the entire previous year.

14. SUBJECT TERMS
IATAC Collection, information assurance, networks, systems, security

15. NUMBER OF PAGES
7

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Executive Summary

The Internet and associated electronic communications have become an indispensable tool for both business and government. This technology allows organizations to conduct electronic commerce, provide better customer service, collaborate with remote partners, reduce communications costs, improve internal communication and access needed information rapidly. However, our reliance on a networked electronic society is not risk free. Security breaches, theft of proprietary information, privacy risk, financial fraud, and sabotage of data or networks are emerging threats in our new information age.

Both the number and sophistication of attacks on our information infrastructure have exponentially increased in the last decade. In fact, there have been more reported incidents of network attack in the last quarter of 2000 than in the entire previous year.

In the rush to benefit from using this new technology, organizations ranging from government to business often overlook the risks associated with electronic systems and therefore, have not made sufficient investment in information assurance products and services. Information Assurance (IA) is the information operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Engineering practices and technology cannot produce systems that are totally immune to attack, but the risks can be reduced and made manageable. Most network and system operators do not have the resources or technical expertise to defend against attacks and minimize damage. Information security and critical infrastructure protection practices and policies are underdeveloped, poorly disseminated, and erratically followed.

To overcome these current shortcomings the following recommendations for government action are provided:

- Fund demonstration programs on several of the infrastructure domains such as air traffic control, power grid, telecommunications, banking, medical and emergency services.

- Fund research and development programs to address the key issues as identified annually by key government councils such as the Chief Information Officers (CIO) Council.

- Identify, support and reward internal and cross-agency initiatives to build a stronger Federal security infrastructure and adequately “capitalize” this effort.

- Foster cooperative research with our allies and coalition partners.

The Current Policy Framework

The Federal government is becoming increasingly dependent on the electronic environment, especially with the transition to e-government. This includes the Internet as well as the telecommunication and data networks owned, operated or managed by Federal agencies. Driven by an Administration and Congress supportive of moving Government functions and services into the 21st century through business-like e-government processes, these agencies must respond to the needs of the citizens to deliver services in new ways, more quickly and effectively, without compromising security and privacy. Legislation and other policy documents aimed at dealing with security and privacy issues include:

The **Clinger-Cohen Information Technology Reform Act**. This 1996 legislation provided the necessary guidance for the federal government to become Information Technology (IT) enabled, to do capital planning, and to become more businesslike in their approach to providing government services.

The **Government Paperwork Elimination Act (GPEA)** ensures continued movement toward meeting the milestone for a fully enabled electronic government by 2003, which includes the requirement for secure access to government information and services.

The **Government Information Security Reform Act**, enacted as part of the Defense Authorization Act of 2001, adds clarity and emphasis to existing legislation by requiring agencies to conduct security reviews and develop agency wide security programs.

Presidential Decision Directives (PDD) 63. Critical infrastructure protection planning and implementation as presented in PDD-63 are moving forward under the direction and guidance of the National Security Council and its National Coordinator for Security, Infrastructure Protection and Counter-Terrorism Office, with operational support from the Critical Infrastructure Assurance Office. The critical infrastructure protection programs under PDD-63 are the foundation for cross-agency and industry efforts. They include 1) *Prepare and prevent;* plan to identify critical infrastructure assets and interdependencies, and address vulnerabilities. 2) *Detect and respond*; plan to detect attacks and intrusions, develop robust intelligence capability, share attack warnings and prepare capability for response, reconstitution and recovery. 3) *Build strong foundations*; for research and development, to identify and train information security specialists, adopt legislation and appropriate funds, and protect the citizens' privacy and civil liberties.

Office of Management and Budget **(OMB) Circular A-130** and the **National Plan for Information Systems Protection** (along with PDD 63) bring focus to the global nature of the problems facing the United States and highlight the need for a strong public-private partnership. The National Plan is the Federal government's road map for this partnership. Version 2.0 of this national plan is expected in the near future, and will

concentrate on the commercial sector, with a focus on identifying the best commercial security practices and ways to share this information for the benefit of both the commercial and government sectors. The National Plan serves as the basis for the internal and cross-agency outreach initiatives to the private sector.

The above listed legislation appears to empower government to move from the paper-based approaches to a digital approach using the Internet and other electronic networks. Other government guidance mandates planning and assessments in both the information security and critical infrastructure protection areas.

In addition, the executive branch through Executive Orders and Presidential Decision Directives, together with the programs of OMB and the CIO Council, have a taken a proactive approach to helping agencies in the planning and implementation of information assurance and critical infrastructure protection solutions. For example, OMB has issued a series of memorandums providing guidance on reporting incidents to the Federal Computer Incident Response Center.

The beginnings of a Federal security infrastructure are taking form. The baseline capability for information security is in place in most agencies, with many CIO's establishing associate positions for information security management. The CIO Council and OMB have put together the framework for building the security management organization in the agencies. They are encouraging the development of a government-wide security infrastructure to support e-government. The building process has started with the basic security management in the agencies. The security management includes an evaluation process based on policies and standards, an interoperable public key infrastructure for e-government applications, and defensive protection capabilities that protect the systems and the privacy of the information for citizen and government users.

While these efforts are beginning to have a positive impact on agencies and the services they deliver to the citizen, much remains to be done. The Fiscal Year 2001 budget showed improved support and interest from the Congress in both information security for existing systems and programs, as well as new, cross-agency initiatives. However, the resources for supporting these activities still fall woefully short of the funding needed to achieve success. In terms of oversight, audits and reviews by various Inspectors General and the GAO continue to document agencies failing to comply with established guidance.

Current Challenges

Departments and Agencies have embraced the need to improve information security infrastructure, but they continue to struggle with identification of the resources necessary to become fully compliant with legislative intent and security policy guidance. Over the past two years, the OMB has worked closely with agencies to build the processes for determining needed resources and appropriately identifying and reporting on security initiatives. In presenting the Fiscal Year 2001 Budget, OMB worked in conjunction with the agencies and the appropriations committees in Congress to present a complete and coordinated picture of the

Administration's consolidated information security program. In the final analysis, the resulting funding was a significant achievement in building awareness and credibility for government-wide initiatives. But as noted by the GAO, there is a long way to go to achieve the requisite level of security needed to support current e-government initiatives.

The information security language in the Government Information Security Reform Act must be translated to effective and measurable implementation plans and programs. OMB is in the process of completing agency clearance for this guidance. The update to the National Plan for Information Systems Protection and a rewrite of OMB Circular A-130 Appendix III, both currently underway, must be completed quickly and presented to the agencies. Agencies must do a better job in the assessment of critical systems and allocating necessary resources to upgrade information security capabilities. Follow-up reporting, measurement and self-inspection are critical.

Recommendations

Information Assurance is a major challenge that demands tough and unique approaches for solutions. We all agree that the vulnerabilities in our information infrastructure not only create risk for government systems, networks, information and public trust, but also create risk to our economic and national security. We must implement processes to better protect information and information systems that are so necessary to our nation's welfare. Although significant first steps have been taken to create the foundation of an Information Assurance infrastructure, additional action is required.

The Government Electronics and Information Technology Association (GEIA) believes that a set of coordinated and properly funded actions are needed. We believe that it is necessary to increase our knowledge of threats, vulnerabilities, and integrated solutions, and to implement effective, measurable security policies and practices. Government must move beyond the reactive stance to one of total awareness and cooperation. We fully concur that industry must join with the government to address many areas of potential mutual benefit. Because infrastructure attacks that inhibit or delay services to the general public cannot be tolerated, it is recommended that the following actions be taken:

- Fund demonstration programs on several of the infrastructure domains such as air traffic control, power grid, telecommunications, banking, medical and emergency services. These demonstrations will show an integrated approach to assessing the information spectrum, understanding when and how attacks will come, taking proactive measures to inhibit the attacks, and demonstrate in real time the ability to counter the threats and maintain the services. Included in these demonstrations, should be "process" specific ideas, allowing agencies to stand-up an information assurance plan or model, measure its effectiveness, report on the results and request the additional funds necessary to improve and implement the process across the agency. We urge setting the development of 15 demonstration and implementation programs in this area. These practical

demonstration programs (some examples follow) should be selected to show the ability to withstand an attack and continue safe operation:

1. FAA inroute system and airport – Where the attacks will take the form of disrupting the sensor information, infiltrating the telecommunications network, and corrupting the information near the take-off and landing zones.
2. Power grid transfers – The attacks may take the form of re-routing the power from where it is needed to somewhere else or causing false alarms to be generated at high risk power generation plants.
3. Emergency Services –Attacks may seek to misdirect the deployment of emergency services, corrupt the information gathered, and alter suspect/victim information.
4. Federal Agencies involved in tax and benefit payment (such as Internal Revenue Service and Social Security Administration) –Attacks to modify critical electronic information.

- Fund research and development programs to address the issues as identified annually by key government councils such as the CIO Council. While trying to solve the substantial tactical challenges facing us today, we must not fail to address strategic problems that are going to occur in five years and beyond. Groups such as the Defense Advanced Research Projects Agency (DARPA), Air Force Research Laboratory and others are underfunded in this regard. Other emerging problems needing solutions are: intrusion detection and recovery for the wireless grid, collateral information system impacts on operational continuity due to non-computer based attacks, effective use of tactical deception as a defensive measure, real time traceback and identification of intruders, and predictive analysis based on system and network activity and event data.

- Identify, support and reward internal and cross agency initiatives to build a stronger Federal security infrastructure and adequately "capitalize" this effort. Cooperation in protecting the infrastructure is the only effective way to combat this problem. We recommend creation, at the national level, of an Infrastructure Emergency Response Team to be the clearinghouse for assurance information and procedures. The primary focus of this program would be to demonstrate the ability to gather information across the infrastructure and then forecast, adapt, and act against threats to the critical national infrastructure. This is over and above the individual infrastructure programs discussed in the first recommendation. This program will demonstrate the ability to get forecasting information earlier through multiple agency cooperation. We strongly support the National Security Council's plan to split the National Coordinator's role into two separate functions, one for security and infrastructure, and the other for counter-terrorism. This

more concentrated focus should help in achieving the level of coordination and cooperation required for success.

- Foster cooperative research programs with our allies and coalition partners for consistent approaches to legal issues, policing, sharing of key information and coalition operations. Some specific research areas are: Cooperative standards for IA event reporting; response (operational continuity) strategies for coalition systems; vulnerability assessments, impacts and mitigation plans for coalition systems; and cooperative forensic, legal and global infrastructure assurance management tools.

The association has a cadre of experienced information assurance professionals with real world knowledge and experience who are willing to help create this partnership. We at the GEIA developed the first technology forecast for information assurance as early as 1996 and have been forecasting the economic growth of the IA sector for several years. In short, our membership understands this technology and is on the front line developing new and cutting edge approaches to solving the information assurance problem. On behalf of the Government Electronics and Information Technology Association membership, we offer you our unbiased, technical assessment of current technologies, as well as promising technologies of the future, to directly support the government in addressing and attacking these challenges.